EBIB Biuletyn EBIB, nr 1 (163)/2016,
Prywatność w bibliotece
Artykuł

Michał „rysiek” Woźniak
Koalicja Otwartej Edukacji

Biblioteki a prywatność

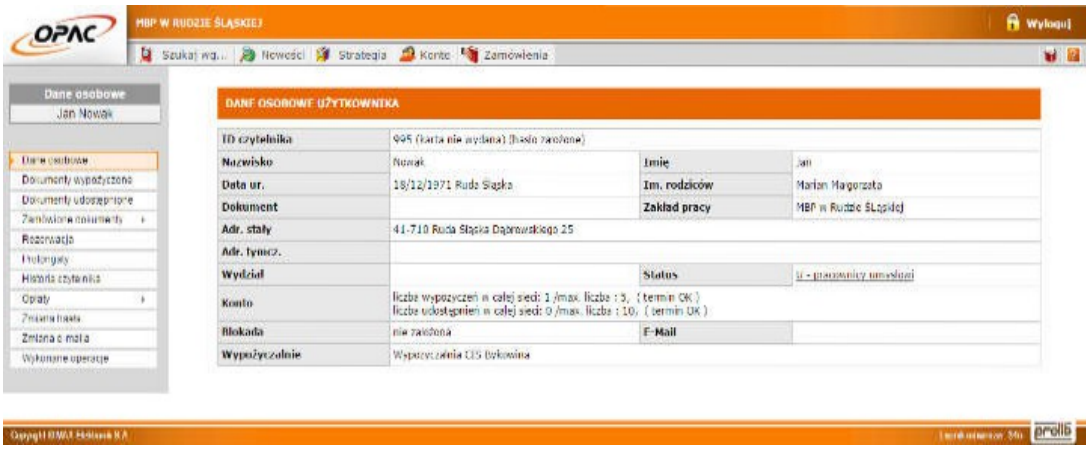
Streszczenie: Autor zastanawia się nad ochroną prywatności i danych osobowych w bibliotekach, nad zagrożeniami pozyskiwania takich danych i wykorzystywaniem ich do celów np. komercyjnych. Wskazuje na grupy hakerów, które mogą być partnerami współpracy dla bibliotek w zakresie pogłębiania wiedzy o ochronie danych czytelników. Przedstawia narzędzia do ochrony prywatności, z których biblioteki mogą skorzystać.

Słowa kluczowe: haker, dane osobowe użytkowników bibliotek, ochrona danych, wykorzystanie danych, Projekt TOR

Wydawać by się mogło na pierwszy rzut oka, że prywatność z bibliotekami wiele wspólnego nie ma. Gdzie wszak, z wyjątkiem tzw. miejsc ustronnych, miałaby się realizować? Już w samej nazwie instytucji nierzadko figuruje słowo „publiczna”, sugerując niejako charakter przestrzeni, w której… No właśnie. W zasadzie nie za bardzo wiadomo, jak skończyć to zdanie. Przestrzenią *stricte* prywatną biblioteka nie jest, to jasne — ale rozbudowanego nadzoru też się w niej nie spodziewamy.

Oczywiście pewne rzeczy nadzorowi w bibliotece podlegają, ale nikt chyba nie będzie zgłaszał obiekcji wobec katalogu bibliotecznego i danych wokół niego gromadzonych (choć w znajdującej się w nim historii naszego czytelnictwa zapisane są przecież nasze gusta) czy wobec uwag dotyczących ewentualnych prób wyniesienia (przez roztargnienie, choćby) pozycji bibliotecznych czy odnotowania tego faktu w bazie czytelników pod warunkiem, że dane są pod kontrolą biblioteki.

Przykładowe dane, jakie gromadzi się w bazach czytelniczych:



II. 1. Jak założyć konto czytelnika w OPAC WWW?
Źródło: Instrukcja Miejskiej Biblioteki Publiczna w Rudzie Śląskiej [on-line] [dostęp 05.012016]. Dostępny w: http://biblioteka.r-sl.pl/biblioteka/index.php/katalog_on-line_instrukcja.html.

Samo nazwanie tych całkiem naturalnych elementów funkcjonowania biblioteki „nadzorem" budzić musi pewien słuszny sprzeciw. Dostęp do danych osobowych powiązanych z katalogiem bibliotecznym ma wszak tylko zespół biblioteki, którego zainteresowanie naszymi preferencjami czytelniczymi zaczyna i kończy się na pytaniu, czy może zamówić kolejną pozycję z pochłanianej przez nas serii lub na ewentualnej życzliwej sugestii kolejnego wartego poznania tytułu lub autorów.

A jednak jeszcze nie tak dawno — jedno pokolenie temu — treść historii czytelniczej pani Kowalskiej czy pana Nowaka mogła być niezmiernie zajmującą lekturą dla osób niekoniecznie z biblioteką związanych (choć mogących uzyskać dostęp do modułów zawierających dane osobowe); na tyle zajmującą w istocie, że osoby te mogłyby nawet chcieć zawrzeć bliższą znajomość z pp. Kowalską czy Nowakiem i to niekoniecznie przy kawie.

Nagle słowo „nadzór" nie wydaje się tak bardzo nie na miejscu, a zmieniliśmy wszak jedynie osoby mające dostęp do gromadzonych informacji i kontekst. Wystarczy ta drobna zmiana, by okazało się, że prywatność była, jest i będzie w bibliotekach sprawą żywą.

O ile nie musimy się na szczęście obawiać wizyty tak specyficznych, stereotypowo ubranych w szare płaszcze, kapelusze i ciemne okulary, czytelników, to pamiętać trzeba, że demokracja nie jest dana raz na zawsze. Co dziś jest niewinną daną zapisaną w katalogu bibliotecznym lub pamięci komputera, jutro może być informacją interesującą nie tylko dla bibliotekarzy. Co nie oznacza, że również dziś nikt nie próbuje uzyskać informacji o czytelniczych gustach. Wprost przeciwnie!

Czasy się zmieniły, zmieniły się metody, zmienił się też cel (walkę z „zaplutym karłem reakcji" zastąpiła próba dotarcia do konsumenta), wciąż jednak kluczem jest zdobycie informacji. Informacji, której źródłem może być biblioteka. Dziś zamiast uzyskiwać dostęp do katalogu kartkowego i kart czytelniczych, można bibliotece zaoferować wygodną usługę „w chmurze" — czyli na serwerze i pod kontrolą usługodawcy. Może to być katalog elektroniczny, może być to przestrzeń do przechowywania plików, ale może to być również narzędzie do analityki odwiedzających stronę biblioteki lub element do umieszczenia na stronie (jak przycisk „Lubię to").

Kto ma wtedy dostęp do historii pp. Kowalskiej i Nowaka? W jakim celu ją wykorzysta? Czy p. Kowalska, czytelniczka książek podróżniczych, dostanie zniżkę na bilet lotniczy? Czy ubezpieczyciel p. Nowaka podniesie składkę ze względu na jego niezdrowe zainteresowania kulinarne? Tak czy owak ani pani Kowalska, ani pan Nowak zapewne nie przewidzieli, że informacje o ich wizytach w bibliotece czy na jej stronie mogą trafić gdzieś poza instytucję.

Nie wynika to wszakże ze złej woli bibliotekarek i bibliotekarzy! Nasi internetowi „nadzorcy" nie szczędzą sił ni środków na tworzenie nowych, coraz lepiej i skuteczniej śledzących nas narzędzi, ukrytych pod płaszczykiem nowych, coraz wygodniejszych funkcjonalności. I o ile nie brak środków na promocję nowych narzędzi ICT wśród bibliotek, zastanawiający

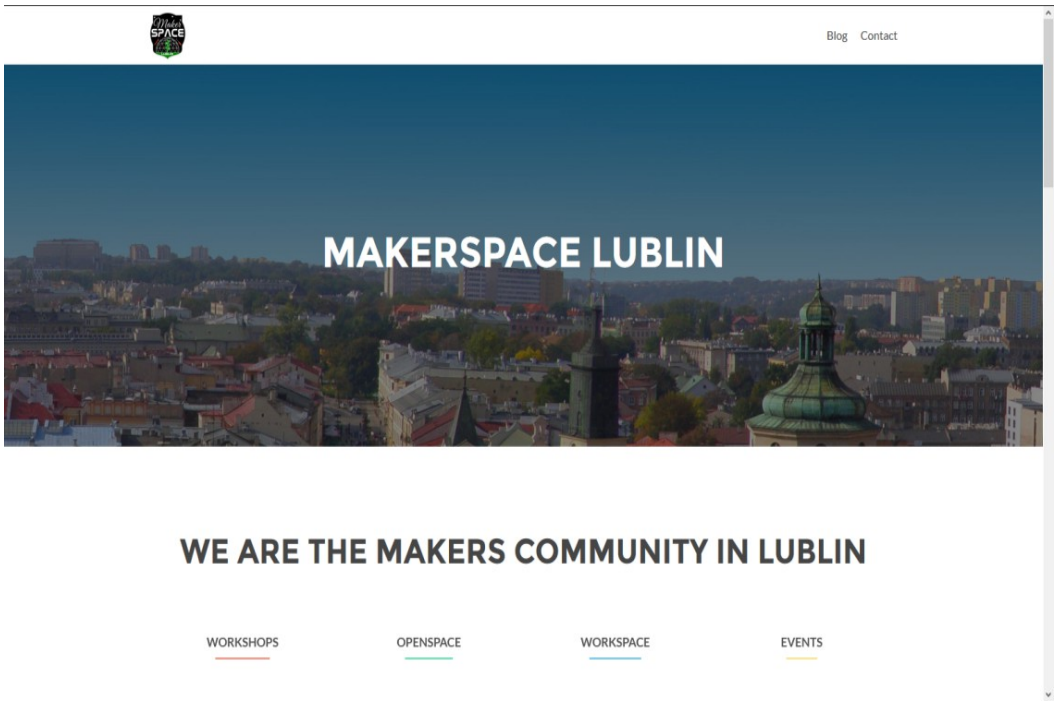
jest niemal zupełny brak środków na podnoszenie kompetencji medialnych, które pomogłyby rzetelnie oceniać koszta różnych rozwiązań nie tylko w wymiarze finansowym, lecz również w wymiarach bardziej miękkich. Jak ograniczenie prywatności na przykład.

Nie jesteśmy jednak w tej grze skazani na porażkę. Możemy preferować narzędzia pozwalające nam zachować kontrolę nad danymi naszymi i naszych czytelniczek i czytelników. Możemy udostępnić naszym odwiedzającym materiały dotyczące prywatności, kompetencji medialnych i poruszania się w cyfrowym świecie. Możemy też pójść krok dalej i dołączyć do grupy bibliotek na świecie, które zdecydowały się stać się częścią sieci Tor, umożliwiającej faktycznie anonimową komunikację w Internecie.

Możemy, wreszcie, nawiązać współpracę z osobami zrzeszonymi w hakerspejsach – klubach majsterkowicza ery cyfrowej. Hackerspace, makerspace, fablab — są to kluby, w których spotykają się i współdziałają makerzy i hakerzy, czyli osoby technicznie uzdolnione, potrafiące swoją wiedzę zastosować w niestandardowy, nieoczywisty sposób. Pomoc takich życzliwych hakerów (nie każdy ślusarz to włamywacz, nie każdy haker to cyberprzestępca) może okazać się nieoceniona, choćby w organizowaniu ciekawych dla młodzieży wydarzeń związanych z prywatnością.

Kluby działają w większości dużych miast Polski, powstają też nowe. Zwykle znajdują się w nich osoby chętne do pomocy w kwestiach technicznych czy dotyczących prywatności, warto więc zastanowić się nad nawiązaniem kontaktu z pobliskim hackerspejsem lub makerspejsem. Część z nich organizuje mniej lub bardziej regularnie spotkania CryptoParty. Oto lista takich organizacji i miejsc:

1. Hackerspace Warszawa https://hackerspace.pl/ kontakt@hackerspace.pl.
2. Makerspace Warszawa http://makerspace.pl/ kontakt@makerspace.pl.
3. Hackerspace Kraków http://hackerspace-krk.pl/ info@hackerspace-krk.pl.
4. Makerspace Lublin http://makerspace-lbn.pl/ fundacja@makerspace-lbn.pl.
5. Katowice Hackerspace Silesia https://hs-silesia.pl/ info@hs-silesia.pl.
6. FabLab Łódź http://fablablodz.org/ http://fablablodz.org/kontakt/.
7. Hackerspace Wrocław https://www.hswro.org/ kontakt@hswro.org.
8. Hackerspace Opole http://hsopole.pl/ hsopole@gmail.com.



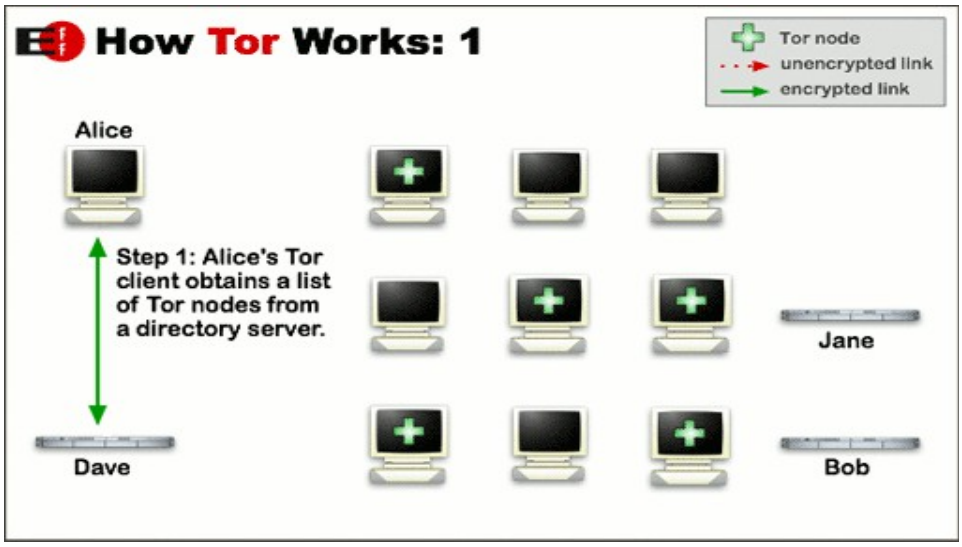
II. 2. Makerspace Lublin .
Źródło: Makerspace Lublin [on-line] [dostęp 04.01.2016]. Dostępny w: http://makerspace-lbn.pl/.

Biblioteki zawsze były magicznymi miejscami, dzięki którym poznawało się świat rzeczywisty lub odpoczywało od niego nieco w świecie przedstawionym. Ta magia, ten tajemniczy ogród wyobraźni wart jest ochrony przed zimnym okiem podglądacza.

Narzędzia do ochrony prywatności

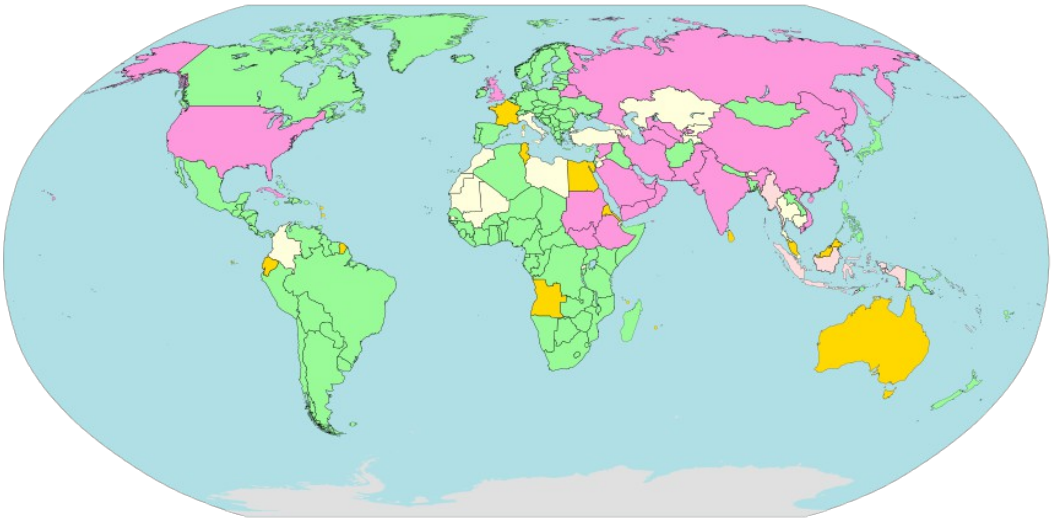
Narzędzia anonimizujące ruch w sieci mają złą prasę. W mediach prawie nie wymienia się ich nazw w kontekście innym niż dotyczącym dostępu do nielegalnych treści, zaś stróże prawa traktują je jak skrzyżowanie dżumy z cholerą. Są one tymczasem nieocenione, jeśli chodzi o unikanie szpiegowania (czy to przez korporacje, czy przez zatroskane o nas rządy) oraz radzenie sobie z internetową cenzurą. A zatem w zasadzie nieodzowne w dzisiejszym, post-Snowdenowskim Internecie.

By działać, narzędzia takie (jak najpopularniejszy z nich Tor, https://pl.wikipedia.org/wiki/Tor_(sieć_anonimowa) muszą być uruchomione w jak największej liczbie miejsc w sieci. Opierają się one bowiem na przekazywaniu ruchu ich użytkowniczek i użytkowników pomiędzy swoimi losowymi węzłami. Uniemożliwia to, lub przynajmniej bardzo utrudnia, określenie, kto komunikuje się z jakim serwerem oraz w praktyce usuwa możliwość cenzurowania połączeń.



Il. 3. Schemat działania Tor.
Źródło: TOR Project. The solution: a distributed, anonymous network [on-line] [dostęp 09.01.2016]. Dostępny w: https://www.torproject.org/about/overview#thesolution.

Jako instytucje o nieposzlakowanej opinii biblioteki mają cenną pozycję pozwalającą angażować się w działania pomagające internautkom i internautom na całym świecie lepiej dbać o prywatność, a obywatelom reżimów cenzurujących dostęp do globalnej sieci (jak Chiny, Iran, USA czy Wielka Brytania) — możliwość obejścia tej cenzury.



Legenda: Cenzura internetu według Reporterów Bez Granic: Wszechobecna cenzura; Znaczna cenzura; Selektywna cenzura; Internet pod nadzorem; Brak dowodów na cenzurę; Brak danych.

Il. 4. Mapa cenzury internetu na świecie.
Źródło: OGDEN, J. (W163). Internet censorship and surveillance world map [on-line] [dostęp 09.01.2016]. Dostępny w: https://commons.wikimedia.org/wiki/File:Internet_Censorship_and_Surveillance_World_Map.svg#/media/File:Internet_Censorship_and_Surveillance_World_Map.svg.

I faktycznie biblioteki to robią. W Stanach Zjednoczonych powstał pomysł Library Freedom Project, w ramach którego m.in. uruchamiane są węzły sieci Tor w amerykańskich bibliotekach. Nie obyło się rzecz jasna bez problemów: na wieść o planie uruchomienia węzła w bibliotece miasta Lebanon w stanie New Hampshire amerykański odpowiednik naszego MSWiA skontaktował się z lokalną jednostką policji, by razem próbować wywrzeć presję na bibliotekę[1] i włodarzy miejskich, poprzez „ostrzeżenie", że Tor może być użyty do niecnych celów.

Il. 5. Logo Library Freedom Project.
Źródło: Introducing LFP's Intern [on-line] [dostęp 09.01.2016]. Dostępny w: https://libraryfreedomproject.org/.

Dyrektor biblioteki początkowo presji uległ, jednak po wsparciu i pozytywnym odzewie społeczności internetowej i obrońców praw człowieka[2] zorganizowane zostało publiczne wysłuchanie, na którym mieszkańcy Lebanon w ogromnej większości zdecydowanie opowiedzieli się za uruchomieniem i utrzymaniem węzła. Mało tego, dziesiątki innych bibliotek w Stanach Zjednoczonych i za granicą skontaktowało się z biblioteką w Lebanon, Library Freedom Project oraz Projektem Tor, pytając jak mogą uruchomić podobne węzły u siebie. W kraju o tak głębokich tradycjach wolnościowych jakim jest Polska, pewnie również znajdą się biblioteki zainteresowane tego rodzaju wsparciem wolności myśli i sumienia w domenie cyfrowej.

Uruchomienie węzła sieci Tor nie wiąże się z dużymi nakładami sił i środków — jeśli mamy dostęp do serwera (czyli po prostu komputera na stałe podłączonego do Internetu i działającego przez większość czasu bez wyłączeń), możemy taki węzeł uruchomić. Ważne jest, by pamiętać o zablokowaniu ruchu wychodzącego poza sieć Tor, możemy bowiem nie chcieć tłumaczyć stróżom prawa, czemu nasz adres sieciowy pojawił się w kontekście dostępu do takich czy innych nielegalnych treści w sieci. W ten sposób staniemy się węzłem pośredniczącym. Uruchomienie węzła niepozwalającego na wyjście poza sieć Tor jest bardzo cenne dla całego projektu, a oszczędza potencjalnie nieprzyjemnych sytuacji.

---

1 GLASER, A., MACRINA, A. *How a small New Hampshire Library fought government fearmongering* [on-line] [dostęp 09.01.2016]. Dostępny w: http://www.slate.com/blogs/future_tense/2015/09/16/how_new_hampshire_s_lebanon_libraries_fought_back_against_dhs_fearmongering.html.

2 *Support Tor and intellectual freedom in libraries. Apel wsparcia z 15 września 2015 r.* [on-line] [dostęp 09.01.2016]. Dostępny w: https://act.eff.org/action/support-tor-and-intellectual-freedom-in-libraries.

Oczywiście można być odważniejszym i zdecydować się zostać węzłem umożliwiającym wyjście poza Tor. Twórcy projektu udostępniają poradnik[3], jak radzić sobie z ewentualnymi problemami ze stróżami prawa w sytuacji, gdy ktoś korzystając z naszego węzła, skorzysta z treści, do których dostęp jest nielegalny. Poradnik jest osadzony w prawie amerykańskim, ale zasadnicze kwestie pozostają bez zmian.

Jeśli biblioteki potrzebują pomocy w uruchomieniu węzła TOR, mogą odezwać się do dowolnego z działających w Polsce hackerspace'ów, lub napisać na adres cryptoparty@hackerspace.pl. Powinno się udać nawiązanie kontaktów z przyjaznymi hakerami, chętnymi pomóc w szczytnym celu.

A przy okazji, nie mniej ważną częścią Library Freedom Project jest organizowanie w bibliotekach spotkań na temat prywatności i szyfrowania, pomagających osobom niezaprzyjaźnionym z techniką poznać metody dbania o swoje bezpieczeństwo i higienę informacyjną w sieci (i poza nią) przez uczenie, jak korzystać z sieci Tor. Mam nadzieję, że takie inicjatywy znajdą swoich realizatorów w naszym kraju.

Bibliografia:

1. *Jak założyć konto czytelnika w OPAC WWW? Instrukcja Miejskiej Biblioteki Publiczna w Rudzie Śląskiej* [on-line] [dostęp 05.01.2016]. Dostępny w: http://biblioteka.r-sl.pl/biblioteka/index.php/katalog_on-line_instrukcja.html.
2. *Makerspace Lublin* [on-line] [dostęp 04.01.2016]. Dostępny w: http://makerspace-lbn.pl/.
3. *TOR Project. The solution: a distributed, anonymous network* [on-line] [dostęp 09.01.2016]. Dostępny w: https://www.torproject.org/about/overview#thesolution.
4. OGDEN, J. (W163*). Internet censorship and surveillance world map* [on-line] [dostęp 09.01.2016]. Dostępny w: https://commons.wikimedia.org/wiki/File:Internet_Censorship_and_Surveillance_World_Map.svg#/media/File:Internet_Censorship_and_Surveillance_World_Map.svg.
5. GLASER, A., MACRINA, A. *How a small New Hampshire Library fought government fearmongering* [on-line] [dostęp 09.01.2016]. Dostępny w: http://www.slate.com/blogs/future_tense/2015/09/16/how_new_hampshire_s_lebanon_libraries_fought_back_against_dhs_fearmongering.html.
6. *Support Tor and intellectual freedom in libraries. Apel wsparcia z 15 września 2015 r.* [on-line] [dostęp 09.01.2016]. Dostępny w: https://act.eff.org/action/support-tor-and-intellectual-freedom-in-libraries.
7. *Electronic Frontier Foundation (EFF). The Legal FAQ for Tor Relay Operators* [on-line]. Last updated April 21, 2014 [dostęp09.01.2016]. Dostępny w: https://www.torproject.org/eff/tor-legal-faq.html.en.

Woźniak, M. Biblioteki a prywatność. *Biuletyn EBIB* [on-line] 2015, nr 1 (163), *Prywatność w bibliotece.* [Dostęp 25.02.2016]. Dostępny w: http://open.ebib.pl/ojs/index.php/ebib/article/view/410. ISSN 1507-7187.

[3] *Electronic Frontier Foundation (EFF). The Legal FAQ for Tor Relay Operators* [on-line] Last updated April 21, 2014 [dostęp 09.01.2016]. Dostępny w: https://www.torproject.org/eff/tor-legal-faq.html.en.